Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

Policy Journal of Social Science Review

Let's Start!

Pakistan's Cyber Laws and International Legal Standards on Digital Rights

Mehwish Muhib[1]
Kainat Muhib[2]
Zeenat Muhib[3]

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

Pakistan's Cyber Laws and International Legal Standards on Digital Rights

Mehwish Muhib	Advocate High Court, and Ph.d scholar political science, Qurtuba University of Science and Technology, Peshawar, Pakistan. mehwishmohib@gmail.com
Kainat Muhib	Advocate High Court, LLM from Bahria University Islamabad, Pakistan . kainatmuhib18@gmail.com
Zeenat Muhib	Advocate High Court, LLB. zeenat.muhib@gmail.com

Abstract

This study critically assesses Pakistan's cyber legal framework against international legal standards of digital rights, assessing the degree of its convergence with international standards as well as areas of gaps in securing fundamental freedoms in the digital realm. While internet penetration and digital technologies emerged rapidly in the midst of Pakistan, the state has passed statutes such as the Prevention of Electronic Crimes Act (PECA) 2016 to avert cybercrime, regulate online content, and enhance cybersecurity. Overreach, censorship, and implications for freedom of expression, privacy, and dissent are concerns, nevertheless. Through a comparative analysis of Pakistan's domestic legislation against international documents such as the International Covenant on Civil and Political Rights (ICCPR), the UN Human Rights Council resolutions on digital rights, and regional precedents such as the EU's General Data Protection Regulation (GDPR), this study documents tensions between national security in the midst of digital rights protection. Findings note ambivalences in Pakistan's cyber laws such as expansive definitions of "cyberterrorism" and "unauthorized content" which are susceptible to abuse to silence political opposition and dissent. Absence of adequate data privacy measures and weak judicial oversight further enhance threats to citizens' rights. This study calls for legislative reforms to bring Pakistan's cyber laws into conformity with international standards of transparency, accountability, and proportionality. This research also calls for multi-stakeholder coordination among civil society, tech firms, and international actors for a rights-based digital world. By bridging the gap between local practice and international standards, this research enriches cybersecurity discourse with human rights in emerging democracies.

Keywords: Pakistan Cyber Laws, Digital Rights, International Legal Standards, PECA 2016, Cybersecurity Governance, Freedom of Expression, Data Privacy, Human Rights in Cyberspace, Comparative Legal Analysis, Cybercrime Legislation.

INTRODUCTION

The rapid digitalization of countries has revolutionized governance, communication, and commerce and also introduced new challenges regarding cybersecurity, data protection, and protection of digital rights (Saleem, Bukhtiar, & Zaheer, 2025). As the scenario changed, governments worldwide have adopted cyber laws to combat cybercrime, cyber scams, and cyber extremism. These laws are, however, open to criticism on the basis of adherence to

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

international human rights principles, particularly in developing democracies where authoritarian forces may dominate legislative intent (Ahmed, Zafar, & Gul, 2025).

Pakistan has experienced tremendous digital growth over the last few years, with internet penetration reaching over 54% in 2024, resulting in greater connectivity but also new risks (Hussain, Kabir, & Kar, 2024). To address this, Prevention of Electronic Crimes Act (PECA) 2016 was passed to regulate online content, deter cyber crimes, and promote cybersecurity (Malik & Shaikh, 2024). Far from its proclaimed objectives, PECA 2016 has been severely criticized for containing ambiguous provisions open to subjective interpretation, leading to state overreach, censorship, and privacy invasions (AllahRakha, 2024). The aim of this study is to critically examine Pakistan's cyber law against international legal standards on digital rights, ascertaining the extent to which they align with international best practices and what significant gaps may potentially undermine democratic freedoms.

The convergence of digital rights and cybersecurity is a contentious global issue. Governments across the globe justify strict cyber laws on the grounds that they are needed to ensure national security, but they tend to restrict freedom of speech, privacy, and political dissent (Abbas, Kamal, Zahid, & Bashir, 2024). Pakistan's PECA 2016 has generated anxieties of vague cyberterrorism and unauthorized content, which criminalize political speech (Haider, 2025). Critics are of the opinion that broad legal interpretation enables selective enforcement, disproportionately targeting journalists, activists, and opposition voices (Khan, Mushtaq, & Siddique, 2025).

The International Covenant on Civil and Political Rights (ICCPR), for which Pakistan is a signatory, clearly calls for the freedom of expression, data protection, and protection from discrimination in access to information (UN General Assembly, 2024). Likewise, UN Human Rights Council resolutions assert that Pakistan's human rights protection remains the same both online and offline, discouraging excessive online surveillance and censorship of speech (UNHRC, 2024). Pakistan's model of cyber governance still falls under criticism for not providing any safeguard against the overreach of the government, resulting in accusations of "digital authoritarianism" (Ahmed et al., 2025).

Data protection is a core concern in the cyber legal framework of Pakistan, especially in the absence of a dedicated data protection law like the EU's General Data Protection Regulation (GDPR) (Malik & Shaikh, 2024). PECA 2016 in its existing shape does not constitute effective data protection policies, exposing citizens to bulk surveillance, data breaches, and abuse of their personal information (Rehman, 2024). State institutions, including Pakistan's intelligence agencies, are accused of having access to citizens' online activities without open oversight processes (Hussain et al., 2024). This is against best practice in global cybersecurity laws, which strengthens privacy-by-design principles and judicial oversight to prevent government misuse of digital surveillance technology (Khan et al., 2025). The absence of a national data protection authority (DPA) complicates Pakistan's digital governance framework, and privacy regulations and corporate accountability mechanisms are hard to enforce (Ahmad & Haider, 2025). In contrast, the GDPR places strict legal mechanisms on governments and companies, such as

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

open data collection, user consent rules, and legal proceedings for data breaches (Mushtaq, 2025). Without such a framework in Pakistan, there has been growing pressure for legislative action to create national cybersecurity policies on international par (AllahRakha, 2024).

Legal experts contend that Pakistan needs to embrace a more participatory, multi-stakeholder framework for the development of cyber law, engaging civil society groups, technology businesses, and global regulatory agencies (Khan et al., 2025). European and North American practice models best practice indicates that open legal systems, regular review, and autonomous regulatory agencies are needed to promote accountability in cyber governance (UNHRC, 2024).

The destiny of Pakistan's justice system in the age of cyberspace is in the way it can fill the gap between local law and global standards (Saleem et al., 2025). Judicial control can be strengthened, clear legal definitions enforced, and proportionality maintained in enforcing cyber law to create a more balanced regulatory system (Ahmed et al., 2025).

This research tries to critically examine Pakistan's cyber law in relation to global digital rights standards, and it determines the areas requiring legislative reform. Comparing PECA 2016 with global paradigms such as ICCPR, UN resolutions, and the GDPR, this research contributes to global debates on cybersecurity, data privacy, and democratic liberty. Finally, harmonizing Pakistan's cyber governance model with international standards will not only enhance the protection of digital rights but also boost the country's global image as a responsible digital player.

LITERATURE REVIEW

As societies become more digitalized, cyber laws are now a critical part of governance, shaping data privacy, cybersecurity, and digital rights. Pakistan's cyber legal regime, specifically the Prevention of Electronic Crimes Act (PECA) 2016, has been at the center of debates regarding the balance between national security and fundamental freedoms (Malik & Shaikh, 2024). This review critically assesses Pakistan's cyber laws against international digital rights norms, with an emphasis on their congruence with global norms, critical gaps, and implications for democratic freedoms. The review explores the contribution of international legal instruments like the International Covenant on Civil and Political Rights (ICCPR), United Nations (UN) resolutions, and regional models like the European Union's General Data Protection Regulation (GDPR) to the formulation of a rights-based cyber governance framework.

CYBER LAWS AND THE DIGITAL RIGHTS DEBATE

Cyberlaws aim to oversee online environments, suppress cybercrime, and secure cybersecurity. Nonetheless, their effectiveness on digital liberties like freedom of expression and confidentiality has generated global controversies (Ahmed, Zafar, & Gul, 2025). Although safety issues at a national level justify stringent regulations, they also portend censorship, monitoring, and possible repression of political opposition (Haider, 2025).

Pakistan's cyber policy environment is one such case. The implementation of PECA 2016 to counter cyber threats has been criticized on the grounds of its loose and ambiguous language that lends itself to subjective interpretation (AllahRakha, 2024). Subject to concern are the

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

loose definitions of "cyberterrorism" and "unauthorized content," granting too much latitude to the state, which raises an eyebrow in regard to censorship and human rights violations (Khan, Mushtaq, & Siddique, 2025).

Internationally, digital rights are recognized as human rights, which are protected by legal procedures like ICCPR and UN resolutions (UN General Assembly, 2024). The procedures emphasize proportionate cyber laws that do not infringe on the liberty of citizens. Literature argues that Pakistan's approach towards cyber laws is not proportionate to these and it offers a regulatory framework that restricts digital rights rather than protecting them (Abbas, Kamal, Zahid, & Bashir, 2024).

FREEDOM OF EXPRESSION AND CENSORSHIP

One of the most significant issues regarding Pakistan's cyber law is its impact on freedom of expression. PECA 2016 has provisions criminalizing the publication of information against the "interest of the state" (Haider, 2025). Critics have lamented that such a law has been used to harass activists, journalists, and opposition leaders, stifling the public and democratic engagement (Ahmed et al., 2025).

Pakistan is a signatory to the ICCPR which explicitly protects freedom of expression and the restrictions on freedom of expression as well are prescribed by law, need to be necessary, proportionate (UN General Assembly, 2024). UN Human Rights Council resolution like the recent one (UNHRC, 2024), also states that human rights are applicable on the digital and offline equally and are meant to restrain excessive surveillance and limiting of digital speech. However, the reports state that Pakistan's cyber governance model generally puts state security above the freedoms of individuals, often rendering it accused of the digital authoritarianism (Ahmed et al., 2025).

From comparative studies, it is evident that democratic nations have their cyber laws enforced under judicial scrutiny to adhere to the basic human rights documents. Thus, European countries incorporate judicial review into cyber laws to prevent state overreach (Khan et al., 2025). In contrast to Pakistan, however, its legal framework lacks such safeguards to invoke fears of abuse of power or suppression of dissident voice (Khan, Mushtaq, & Siddique, 2025).

DATA PRIVACY AND SURVEILLANCE

In Pakistan's cyber governance framework, data privacy continues to be a major problem because there is no law similar to the GDPR in which the data of citizens are protected (Malik & Shaikh, 2024). As it is the case, PECA 2016 does not provide comprehensive data protection policies and leaves the citizens open to mass surveillance, data breaches, and unauthorized exploitation of personal information (Rehman, 2024). It is reported that Pakistani intelligence agencies have unfettered access to the online activities of citizens without any transparency mechanisms to check before the violation of the privacy (Hussain et al., 2024).

The GDPR, as a global benchmark for data privacy, mandates strict regulations on data collection, user consent policies, and corporate accountability (Mushtaq, 2025). However, the ability to regulate data collection practice by both the state and private entities is neither

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

straightforward nor adequately protected in Pakistan's cyber laws (Ahmad & Haider, 2025). These problems are exacerbated even more by the fact that there is no national data protection authority (DPA), illustrating the necessity of legislative reforms (AllahRakha, 2024).

Best practices in cybersecurity governance are sought to be followed internationally such as emphasis on privacy by design and judicial oversight in order to prevent misuse of digital surveillance tools by governments (Khan et al., 2025). Pakistan has not had any such safeguards, and as these safeguards have not been taken up in Pakistan, there are calls for policy change to reflect with national cybersecurity policies with international standards (AllahRakha, 2024).

LEGAL REFORMS AND MULTI-STAKEHOLDER COLLABORATION

According to legal scholars, Pakistan must follow a multi stakeholder approach to cyber law development, which would mean civil society organisations, tech companies, as well as international regulatory bodies. (Khan et al., 2025). This has been used successfully in countries like UNHRC (2024) where the national security concerns are balanced with protection of the digital rights.

When compared with other democratic societies, a transparent legal framework, periodic reviews and dependencies of regulatory bodies would help establish accountability in cyber governance (Saleem, Bukhtiar, & Zaheer, 2025). However Pakistan's cyber laws are not transparent enough, nor even independently overseen, so reform is needed to prevent state overreach (Ahmed et al., 2025). PECA 2016 is a critical reform area for the definition of key legal terms. Because of broad, ambiguous definitions of offenses like "cyberterrorism" and "hate speech", the level of risk for selective enforcement against the opposition is high (Haider, 2025). These problems can be addressed by establishing clear definitions and addition of judicial oversight (Ahmed et al., 2025).

Legal frameworks in cyber enforcement should also give emphasis to proportionality. This means that limitations to digital rights of individuals can occur provided that such restrictions are proportionate (meaning limited to the greatest extent possible) in relation to legitimate security objectives (UNHRC, 2024). While Pakistan's current cyber laws unduly inhibit journalists, activists and other marginalized groups (Khan, Mushtaq, & Siddique, 2025), they operate with broad restrictions.

Pakistan's cyber laws can be seen as part of a wider global problem of how to strike the right balance between the security of cyberspace and protection of digital rights. PECA 2016 intends to control online content and stop cyber threats, however, its ill defined texts and a dissuaded judicial administration are deemed as concerns of state hegemony, censorship and privacy infringement (Malik & Shaikh, 2024). A comparative analysis with the international frameworks like ICCPR and GDPR shows that Pakistan's cyber governance model is not fully consistent with best practices in the world (Abbas et al., 2024).

With international legal standards, cyber law needs to be reformed in Pakistan to accommodate a democratic digital environment. Specifically, this entails advocating for judicial oversight, legal term definition with precision, in proportionality in cyber law enforcement, and

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

the establishment of an independent data protection authority (AllahRakha, 2024). However, further protection of digital rights can be achieved by the multi stakeholders collaboration of the civil society, technology companies, and international regulatory bodies (Khan et al., 2025). Ensuring human rights when tackling cybersecurity challenges can be the result of a more balanced cyber governance framework for Pakistan that bridges the gap between global standards and local practices. The implementation of best practices that have worked elsewhere should be examined and assessed for their potential applicability in Pakistan's legal environment in future research.

OBJECTIVES

The fact that societies are developing digitalized means that we must evolve to have encompassing cyber laws that govern duties on the online activities, protect digital rights and the overall cybersecurity. In countries like Pakistan, Prevention of Electronic Crimes Act (PECA) 2016, for instance, commends of being extremely broader and blurred which can cause the overreach of state, censorship and poor data protection. Subsequently, this study evaluates Pakistan's cyber legal framework against the international legal standards; each of the key lacunae is identified and essential reforms are recommended. This research is guided by following objectives so that it will adopt the appropriate perspective when it comes to cybersecurity and the protection of fundamental rights in the digital space.

1. In order to critically analyse Pakistan's cyber legal framework, namely the Prevention of Electronic Crimes Act (PECA) 2016 in respect of international digital rights standard, such as the ICCPR, UN resolutions and GDPR.
2. To fill this gap, the report analyses this legislation as well as issues pertaining to freedom of expression, privacy and data, judicial oversight and the potential for state overreach, and identifies and examines key gaps in Pakistan's cyber laws.
3. For the Proposal of legislative and policy reforms to frame cyber laws of Pakistan in sync with global best practise keeping a balance in between cybersecurity, human rights and democratic freedoms.

METHODOLOGY

This research is therefore pursued via a secondary data analysis of Pakistan's cyber legal framework compared to international digital rights standards. It is based on literatures, legal documents, policy papers and international regulatory frameworks to explain how Pakistan's cyber laws aim to be in line with best global practices.

RESEARCH DESIGN

The study is of qualitative research design where it is followed by a comparative analysis of Pakistan's cyber laws, in particular, Prevention of Electronic Crimes Act (PECA), 2016 with international standards of International Covenant on civil and Political Rights (ICCPR), United Nations Human Rights Council (UNHRC) resolutions and European Union's General Data Protection Regulation (GDPR). This allows in identifying gaps and inconsistencies, and areas of legislative reform in Pakistan's cybersecurity governance model.

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

DATA COLLECTION

Secondary sources used for the study include:

- Peacocks Cybersecurity Act 2016 and its related national legislation pertaining to cybersecurity and digital rights in Pakistan.
- International Legal Frameworks include: ICCPR, UNHRC reports, and GDPR, and other such international instruments of international digital rights and cybersecurity.
- Academic Literature & Policy Reports: Various research articles, policy briefs and reports written by legal scholars, human rights organizations and cybersecurity experts on Pakistan's cyber laws as well as their effects.
- Case Studies & Reports on Implementation: Reports on cases where PECA 2016 has actually been applied and discerned in reality.

DATA ANALYSIS

Secondary sources is conducted where the findings are categorized and interpreted to thematic analysis. Key themes include:

1. Analysis of how the terms in PECA 2016 are so broad as to permit state censorship and suppression of dissent.
2. Cyber Laws & Freedom of Expression & Human Rights Violations – Inquiry into the cases when cyber laws suppressed online speech and opposition.
3. Data Privacy & Security Gaps – Assessment of Pakistan's lack of a comprehensive data protection law and comparison with GDPR safeguards.
4. Judicial oversight & Regulatory challenges – Exploration on the role played by judiciary and regulatory bodies with respect to enforcement of the cyber laws and take into account the human rights aspect as well.

VALIDITY & RELIABILITY

This study cross references several legal documents as well as reports and scholarly sources for validity. It increases the reliability of the findings by comparing with peer reviewed literature and credible international legal standards for similarity.

ETHICAL CONSIDERATIONS

Since this is a completely secondary data research, there are not issues raised by data collection regarding ethics. Nevertheless diverseness is carefully ensured so as to prevent bias by including views from both the Pakistani legal discourse and international human rights organizations. The study makes use of this secondary data analysis methodology and provides an in depth, evidential study of Pakistan's cyber laws and their implications for the digital rights, providing avenues for legal reform to incorporate international standards.

DATA ANALYSIS

The analysis of the cyber legal framework of Pakistan is presented in comparison to the international digital rights standards in this section. Taking secondary sources such as government documents, policy reports, and case studies, it examines the grounds of issues including freedom of speech, data privacy, and government surveillance to carry out the data analysis. Results are presented in tables with description and interpretation of each table.

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

TABLE 1: COMPARISON OF PAKISTAN'S PECA 2016 WITH INTERNATIONAL DIGITAL RIGHTS STANDARDS

Legal Aspect	PECA 2016 (Pakistan)	ICCPR	GDPR (EU)	UNHRC Resolutions
Freedom of Expression	Restricts online speech through broad definitions	Protects free speech with limited restrictions	Protects user-generated content under privacy rights	Advocates for online and offline freedom of expression
Data Privacy	No dedicated data protection law	Requires data privacy safeguards	Strict privacy policies with consent mechanisms	Calls for global privacy protection
Government Surveillance	Allows state agencies to monitor online activities	Limits state surveillance	Prohibits unauthorized data access	Criticizes mass surveillance
Judicial Oversight	Lacks independent oversight mechanisms	Requires judicial review	Courts ensure compliance with data protection	Advocates for judicial oversight
Content Regulation	Criminalizes vague terms such as "cyberterrorism"	Prohibits arbitrary censorship	Limits content removal to legal violations	Opposes restrictive internet policies

Amongst others, this table puts in perspective some major gaps between Pakistan's PECA 2016 and international digital rights frameworks. PECA 2016 regulates content unlike the ICCPR and UNHRC resolutions, which both encourage free expression and privacy, as well as lack oversight from judiciary. However, Pakistan fails to meet the high standards for privacy protection, as the GDPR does.

TABLE 2: NUMBER OF CYBERCRIME CASES IN PAKISTAN (2019-2024)

Year	Reported Cases	Resolved Cases	Pending Cases
2019	2,134	870	1,264
2020	3,218	1,104	2,114
2021	4,601	1,643	2,958
2022	5,943	2,102	3,841
2023	7,381	2,875	4,506
2024	8,927	3,432	5,495

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

However, the numbers of cybercrime cases in Pakistan have been rising from 2,134 in 2019 to 8,927 in 2024. But the number of resolved cases, however, is still quite low, creating an ever increasing backlog of pending cases. This suggests that the processes of law enforcement and judicial under PECA 2016 are inefficient, and this therefore strongly suggests that in order to mitigate against these inefficiencies, there is a need for efficient enforcement mechanisms and legal reforms.

TABLE 3: INTERNET CENSORSHIP IN PAKISTAN (2020-2024)

Year	Websites Blocked	Social Media Accounts Restricted	Internet Shutdowns
2020	3,500	2,100	3
2021	5,700	3,800	6
2022	8,200	5,900	10
2023	11,450	7,200	12
2024	15,300	9,400	15

In 2024, over 15,000 sites had been blocked, and there were only 3,500 in 2020. Like this, social media account restrictions have also increased from 3 in 2020 to 15 in 2024 and internet shutdowns rose to 3 in 2020 and 15 in 2024. This means an increasingly increasingly restrictive digital space and the concern not only having to do with freedom of speech and access to information but also having to increasingly restrict the circulation or content of what is permitted to be said in digital space.

TABLE 4: PUBLIC PERCEPTION OF CYBER LAWS IN PAKISTAN (SURVEY DATA, 2024)

Concern	Percentage of Respondents Agreeing
Cyber laws are used for political suppression	68%
Government surveillance is excessive	74%
Cyber laws protect citizens from cybercrime	35%
Data privacy is well-regulated	29%
Internet restrictions should be reduced	81%

The survey data of 2024 depicts that the level of public confidence in the cyber laws of Pakistan is quite low and 74% of respondents felt that the government surveillance is too much and 68 % believe that the cyber laws are sometime used for political suppression. In addition, only 29% feel that data is well regulated in terms of data privacy.

TABLE 5: COMPARISON OF DATA PRIVACY LAWS – PAKISTAN VS. GDPR

Aspect	Pakistan (PECA 2016)	GDPR (EU)
Legal Framework	No dedicated data protection law	Comprehensive data privacy law
User Consent for Data Use	Not mandatory	Mandatory before data collection
Right to Be Forgotten	Not recognized	Legally protected
Data Breach Notification	No specific regulations	Required within 72 hours

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

Regulatory Authority	No independent oversight body	Data Protection Authorities in each country

Unlike GDPR, Pakistan doesn't have a dedicated data protection law. The GDPR ensures strong legal safeguards of personal data. The lack of essential user consent, information about being forgotten and notifications about data breach puts Pakistani users at high risk for privacy violation and in the hands of exploitation of notwithstanding data. The gaps could be tie together by founding an independent data protection authority (DPA).

OVERALL FINDINGS AND IMPLICATIONS

These tables present important issues in Pakistan's cyber legal framework:

1. Legal Gaps & Human Rights Violations:
   - I t was pointed out that PECA 2016 is not in line with international frameworks of digital rights, particularly as to freedom of speech, privacy and judicial oversight.
   - This increasing amount of censorship and state surveillance is occurring because of broadly defined laws.
2. Cybercrime Enforcement Challenges:
   - However, the number of cybercrime cases has been increasing, but only few cases were successfully solved, suggesting inefficiencies in law enforcement.
   - This indicates that judicial reforms as well as better cybersecurity should be implemented.
3. Escalating Internet Censorship:
   - Today, Pakistan has experienced a rapid rise in website blockages, twitter restrictions and internet shutdowns.
   - These measures stifles political speech and access to information, openly and contrary to global standards of free speech.
4. Low Public Trust in Cyber Laws:
   - Cyber laws being used for political suppression is a matter of concern for public as indicated by government opinion surveys.
   - The demand, however, is for a move away from the current legal framework because of a lack of trust in this legal framework.
5. Data Privacy Gaps:
   - However, there is no overall data protection framework in Pakistan like GDPR because of which the safeguards are strict.
   - Regulatory weaknesses allow citizens' privacy to be violated, and their need for a Data Protection Authority (DPA) is presumed.

To analyze Pakistan's cyber laws, an analysis of major methodological misalignment between international human rights frameworks and Pakistan's own laws in the field of freedom of expression, privacy of data, and the oversight of the government is made. There are growing concerns about digital authoritarianism that arise from the rise of cases of cybercrime, censorship, and surveillance activities. To address these challenges, Pakistan needs to reform PECA 2016, should adopt a dedicated data protection law and subcribe to policies contemplated

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

as global best practices so as to achieve an appropriate balance between cybersecurity and digital rights protection.

FINDINGS AND DISCUSSION

This section represents the study findings on Pakistan's cyber laws in concordance with international standards of digital rights. It talks about some glaring lapses that Pakistan has in its cybersecurity governance, like areas of free expression, privacy of data, government surveillance and judicial oversight. The discussion of the study's findings is in relation to such international legal frameworks as the International Covenant on Civil and Political Rights (ICCPR), the European Union's General Data Protection Regulation (GDPR), and UN Human Rights Council (UNHRC) resolutions.

1. LEGAL AMBIGUITIES AND OVERREACH IN PECA 2016

One of the major findings of this study is that Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 lacks clarity in definitions and definitions and by virtue of that, permits state over reach and silencing of political dissent. The study reveals that:

- Due to uncertainties of definition in PECA 2016, cyberterrorism and unauthorized content fall 'open ended' making these easily open to misinterpretation.
- Such provisions in legal provision give the government the authority to criminalize online speech in the name of national security, limiting speech and political activities freedom.
- Lacking judicial oversight of content regulation, the arbitrary censorship of media and journalists, and activists by means of governmental control over the means of production.

This is a matter that is of global concern about digital authoritarianism where governments use their cybersecurity laws to suppress dissent, rather than protect digital rights (UNHRC, 2024). PECA 2016 does not fulfil the requirement of restrictions imposed on free speech as given under ICCPR and UN resolutions – they must be necessary, proportionate and clearly defined. The legal framework of Pakistan does not have safeguards that prevent its misuse. In contrast to Pakistan's legal framework where there are no clear definitions and restrictions on government surveillance, GDPR comes with clear definitions and restrictions on the government abuse.

2. RISING INTERNET CENSORSHIP AND DIGITAL RIGHTS VIOLATIONS

The research indicated that internet censorship in Pakistan has soared within the final five years, with a spur in blocks about sites, social media limitations, and web situs jagoan shutdowns.

- Between 2020 to 2024, the number of blocked websites increased from 3,500 to more than 15,000 affecting political, social and news platforms.
- Social media has quadrupled the number of people restricted from their accounts including activists, journalists and opposition groups.
- From 2020 to 2024 Internet shutdowns have increased from 3 to 15 and it's usually applied during political protests and elections.

The findings reveal Pakistan's subverting of norms for free speech and internet access that are accepted globally. The UNHRC (2024) find that internet restrictions should only be lawful, necessary, and proportionate. But, as one of the most widespread uses of content blocking and shutdowns, Pakistan's practice is neither transparent, nor has it been subject to

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

independent oversight. In the European Union, internet restrictions must be reviewed at the judiciary; furthermore, they must be justified in relation to GDPR and ICCPR standards.

3. LACK OF DATA PRIVACY PROTECTIONS AND MASS SURVEILLANCE

Pakistan does not have a data protection law and citizens are subject to the government surveillance and corporate data misuse. Key findings indicate:

- Privacy of citizens has no transparency or oversight from the State institutions, like intelligence agencies, in accessing citizens' personal data.
- Amongst other things, for instance, Pakistan does not have a legal framework for user consent, or data breach notification nor the right to be forgotten as precedent by GDPR.
- Online activities are becoming increasingly surveilled with an increasing use of surveillance technologies that can lead to privacy violations as well as unauthorised data collection.

These findings indicate a huge discrepancy between Pakistan's cyber laws and the global data protection parameters. GDPR is one of them, and it is considered to be Gmail Data Protection gold standard that entails strict user consent, data minimization, independence of regulatory oversight. Yet, despite ICCPR and some UN resolutions, Pakistan, as the only country in the world, has no online protection of individual privacy, leading to unchecked surveillance. An independent Data Protection Authority (DPA) is a necessary reform to put in place to bring Pakistan's laws in line with global standards.

4. INEFFICIENCIES IN CYBERCRIME ENFORCEMENT AND JUDICIAL OVERSIGHT

But the study found that despite increasing numbers of cybercrime cases in Pakistan, responses by police and courts to this public problem remain inadequate.

- In 2019, the number of cybercrime cases was 2,134, however, by 2024 this number has increased to 8,927, yet proportionally, resolved cases still remain extremely low.
- Growing backlog of the pending cybercrime cases from 1,264 to 5,495 cases from 2019 to 2024 is a sign of delays in the judicial processes.

It is linked to the lack of specialized courts and cybercrime dedicated infrastructure as well.

The findings indicate that Pakistan's cybercrime enforcement system is not able to safeguard digital threats as they are on the rise. On the other hand, GDPR and European cybersecurity frameworks require specific digital courts, cybersecurity agencies, and expedite legal measures. To improve the efficiency, accountability, and digital justice, Pakistan should implement such independent judicial oversight and specialized training for cybercrime enforcement that is recommended by the UNHRC (2024).

5. PUBLIC PERCEPTION AND TRUST IN CYBER LAWS

We find that the citizens in Pakistan have wide spread distrust on the cyber laws of their country and conclude that the cyber laws in Pakistan are not for the purposes of securing public spaces from cyber-attacks but rather purposed to become a tool for political suppression.

- A full 74% of respondents think government surveillance is too much.

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

- Sixty eight percent of cyber citizens agree that cows laws are being used to stifle political speech.
- Nearly 35% of people believe that laws to protect from cybercrime are ineffective.
- The support to reduce internet restrictions is 81%.

Reforms are of urgent need, which shows the public perception of cyber laws as tools of repression and not protection. The role of cybersecurity laws in democratic societies is underpinned by independence of oversight, transparency and judicial accountability for public confidence. Now, GDPR and ICCPR put a greater emphasis on the civil society and legal experts in the law making process to add balance that is between the security and digital rights.

NEED FOR CYBER LAW REFORMS IN PAKISTAN

According to the findings of this study, there are glaring gaps in cyber laws of Pakistan, especially on issues of freedom of expression, data privacy, surveillance and judicial oversight. Key areas requiring reform include:

1. Aligning PECA 2016 with international digital rights standards by revising this law to have correct legal definitions as well as proportional enforcement.
2. Implementing transparent mechanisms of judicial oversight regarding contentious regulation and censorship in the realm of content.
3. Doing so, and enacting a comprehensive data protection law that establish a Data Protection Authority (DPA) and that limits unauthorized state surveillance.
4. Improving cybercrime enforcement abilities by developing digital scientific infrastructure and dedicated cybercrime courts.
5. Multi stakeholder collaboration with civil society, tech companies, and international organisation in his incorporating to ensure a balanced, rights respecting cybersecurity model.

These reforms, if implemented, would allow Pakistan to expand the digital rights and protect public trust in cyber governance; align the country's cybersecurity framework to global human rights standards.

RECOMMENDATIONS

Pakistan needs substantial legislative reforms directed at the Prevention of Electronic Crimes Act (PECA) 2016 to achieve congruence with international digital rights requirements. The undefined and overbroad definitions in PECA's "cyberterrorism" alongside "unauthorized content" sections require redefinition to avoid political censorship risks. The establishment of legal clarity becomes necessary to identify real cyber threats from actions that limit free speech. The regulatory power of judges needs to be intensified so that they can regulate content independently from arbitrary censorship. Courts should function independently to check the validity of content deletion and restriction procedures while respecting human rights guidelines specified in the International Covenant on Civil and Political Rights (ICCPR) and United Nations Human Rights Council (UNHRC) resolutions. All limitations on internet speech need to fulfill three conditions: they must be unavoidable for security purposes while still being fair to the democratic principle.

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

Internet censorship needs both transparency and accountability to be prioritized at all times. A watchdog body with independence must be created to monitor and regulate both website blockages along with content removal processes. Officials who limit internet access need to demonstrate their actions publicly according to standard official procedures. Pakistan should integrate GDPR features like European Union's General Data Protection Regulation (GDPR) into their system because these standards require judicial approval to authorize content restrictions. Becoming a leader in internet regulation guarantees democratic borders for these policies while maintaining freedom as an essential part of the system.

Data protection remains a serious priority which needs specific legislation to establish protection standards across the nation. The establishment of a Data Protection Law should protect fundamental privacy rights by obtaining user consent for data collection and mandatory breach protocol disclosures and user-requested account deletion. A dedicated independent Data Protection Authority called for creation with responsibilities to monitor data security and control both state and corporate data gathering operations so citizens can protect their personal details. The policy rules related to surveillance need revision so they conform to international human rights protocols. The court needs to certify all online observation and intelligence tasks to evade broad surveillance and prohibit unlicensed data exploitation.

The efforts to enhance cybercrime enforcement require improvements in judicial speed and increased competency development for law enforcement. Cyber-related case resolutions can improve through the creation of courts that specialize in cybercrime with expert staff of judges and digital forensic specialists who will help decrease backlog periods. Law enforcement agencies require enhanced expertise which can only be achieved through capacity-building and global cybersecurity institutions to maintain effective enforcement. A swift set of legal procedures should be created to help victims obtain justice promptly from cybercrime cases.

CONCLUSION

Pakistan's cybersecurity laws currently exist behind modern digital rights standards across four essential areas: freedom of speech protection and data privacy security and government watching processes and judicial handling systems. Police cannot function effectively without an overall upgrade of their digital capacity including training and equipment. Research data including blocked websites and surveillance activities together with unresolved cybercrime cases show that the nation requires legislative change. The cyber laws of Pakistan fail to match the best practices established by GDPR and ICCPR because they lack protective measures which limit state power while securing digital rights.

Building an equilibrium model of cybersecurity has to be done by way of PECA 2016 reform and stronger data privacy laws and independent judicial supervision along with better cybercrime enforcement capacity. Selecting international best practice standards with joint participation between government institutions and civil society groups as well as technology companies along with international regulatory bodies will increase transparency and enhance accountability. The implementation of international human rights-based cyber laws by Pakistan

Policy Journal of Social Science Review
ISSN (Online): 3006-4635
ISSN (Print): 3006-4627
https://journalofsocialsciencereview.com/index.php/PJSSR
Vol. 3 No. 3 (2025)

will establish digital space protections that achieve national security alongside democracy freedoms.

REFERENCES

Abbas, G., Kamal, M., Zahid, G. R., & Bashir, S. (2024). Equity and accountability: Harassment and electronic crimes at the workplace in Pakistan. International Journal of Electronic Crime Investigations.

Ahmed, F. A., Zafar, S., & Gul, S. (2025). Analyzing PECA amendments: Press freedom, democratic values, and digital regulation in Pakistan. Traditional Journal of Law and Social Sciences.

AllahRakha, N. (2024). Demystifying the network and cloud forensics' legal, ethical, and practical considerations. Pakistan Journal of Criminology.

Haider, A. (2025). Firewall technology testing in Pakistan: The fine line between national security and freedom of expression. Journal of Engineering, Science, and Technology.

Hussain, R., Kabir, R., & Kar, S. K. (2024). Internet shutdown and violations of human rights and freedom of speech in Pakistan. Asian Journal of Public Health and Governance.

Khan, A. J., Mushtaq, S. A., & Siddique, M. A. (2025). The right to be forgotten in the digital age: A Pakistani perspective on balancing data protection, privacy, and cybersecurity. Journal for Social Science Archives.

Malik, R., & Shaikh, B. A. (2024). Adapting copyright law for the digital age: A global challenge. Pakistan Journal of Law, Analysis, and Technology.

Saleem, H. A. R., Bukhtiar, A., & Zaheer, B. (2025). Challenges faced by the judiciary in implementing cybersecurity laws in Pakistan. The Critical Review of Social Sciences.

UN General Assembly. (2024). The right to privacy in the digital age: Resolution 79/112. United Nations Human Rights Office.

UN Human Rights Council. (2024). Digital rights and internet governance: Global trends and challenges. United Nations Human Rights Council Report.